Welcome to the PIA for FY 2010!

Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.

To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person.

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

Directions:
VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program. More information can be found by reading VA 6508.

If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.

PIA Website: http://vaww.privacy.va.gov/Privacy_Impact_Assessments.asp

Roles and Responsibilities:
Roles and responsibilities for the specific process are clearly defined for all levels of staff in the Privacy Impact Assessment Handbook 6202.2 referenced in the procedure section of this document.
   a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Handbook 6202.2.

   b. Records Officer is responsible for supplying records retention and deletion schedules.

   c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Handbook 6202.2 and to immediately report all anomalies to the Privacy Service and appropriate management chain.

   d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.

   e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and

systems, coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues, and reviewing and approving the PIA before submission to the Privacy Service.

Definition of PII (Personally Identifiable Information)

Information in identifiable form that is collected and stored in the system that either directly identifies and individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirect indentify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

Macros Must Be Enabled on This Form

To enable macros, go to: 1) Tools > Macros > Security - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on Enable Macros at the prompt.

(FY 2010) PIA: System Identification

Program or System Name: OM>FSC>CCS>

OMB Unique System / Application / Program
Identifier   (AKA: UPID #):   None

The Credit Card System (CCS), is operated and supported by the Financial Services Center (FSC), and is a major application that processes four different types of transaction data for various input interfaces. The types of data include: Prime Vendor, Purchase Card (including Fee Basis and Convenience Check), Fleet, and Centrally Billed Travel. Prime Vendor, Purchase Card, Fleet, and Travel data are received daily in Data Exchange File (DEF) format and are loaded into the CCS Oracle relational database that resides on a Dell PowerEdge 6850 server. The compressed and encrypted files are delivered (continued in Tab 8)

Description of System / Application / Program:

Facility Name: Financial Services Center (FSC)

Title:	Name:	Phone:	Email:
Privacy Officer:	Cathy Brean	512-460-5175	cathy.brean@va.gov
Information Security Officer:	Krystal Johle	512-460-5043	krystal.johle@va.gov

Chief Information Officer:	Larry Sherman	512-460-5300	larry.sherman@va.gov
Person Completing Document:	Lori Thomas	512-460-5189	lori.thomas2@va.gov
Other Titles:	Ed Niedzielski	512-460-3079	edward.niedzielski@va.gov
Other Titles:	None	None	
Other Titles:	None	None	
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	08/2009		
Date Approval To Operate Expires:	Aug-11		

What specific legal authorities authorize this program or system:	This project is authorized under the VA Chief Business Office. To provide the credit Cards to VA users and maintain the transactions data. System of Record cites 5 U.S.C. 552A(e), 31 U.S.C. 3512, 31 U.S.C. 3711, 31 U.S.C. 3721, 5 U.S.C. 5701 et seq., 5U.S.C. 41119b), Pub. L. 97-365, 26 U.S.C. 6103(m)(2), 5 U.S.C., 5514, 31 U.S.C. 3716, 31 U.S.C. 321, 5. U.S.C. 301, 5 U.S.C. 4101 et seq., 41 CFR parts 301-304, EO 11348, and Office of Management and Budget (OMB Circular A-127. Federal Acquistion Regulation (FAR), part 13, 48 CFR part 13, and Public Law 93-579, section 7(b).
What is the expected number of individuals that will have their PII stored in this system:	32,080
Identify what stage the System / Application / Program is at:	Operations/Maintenance

The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.   11 years, 1998

Is there an authorized change control process which documents any changes to existing applications or systems?   Yes

If No, please explain:
Has a PIA been completed within the last three years?   Yes

Date of Report (MM/YYYY):   12/2009

☐ Have any changes been made to the system since the last PIA?

☐ Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?

☑ Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?

☑ Does this system/application/program collect, store or disseminate PII/PHI data?

☑ Does this system/application/program collect, store or disseminate the SSN?

(FY 2010) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records?

Yes

if the answer above is no, please skip to row 16.

For each applicable System(s) of Records, list:

    1. All System of Record Identifier(s) (number):   131VA047

    2. Name of the System of Records: Purchase Credit Card Program

    3. Location where the specific applicable System of Records Notice may be accessed (include the URL):   http://www.rms.oit.va.gov/SOR_Records.asp

Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?	Yes
Does the System of Records Notice require modification or updating?	No
	(Please Select Yes/No)
Is PII collected by paper methods?	Yes
Is PII collected by verbal methods?	No
Is PII collected by automated methods?	No
Is a Privacy notice provided?	Yes
Proximity and Timing: Is the privacy notice provided at the time of data collection?	Yes
Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?	Yes
Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?	Yes
Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?	Yes

(FY 2010) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	VA File Database	Payment of credit charges	Automated	Automated
Family Relation (spouse, children, parents, grandparents, etc)	N/A			
Service Information	N/A			
Medical Information	N/A			
Criminal Record Information				
Guardian Information	N/A			
Education Information	N/A			
Benefit Information	N/A			
Other (Explain)	N/A			

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	VA Files / Databases (Identify file)	Mandatory	
Family Relation (spouse, children, parents, grandparents, etc)	No			
Service Information	No			
Medical Information	No			
Criminal Record Information	No			
Guardian Information	No			
Education Information	No			
Benefit Information	No			
Other (Explain)	No			
Other (Explain)	No			
Other (Explain)	No			

(FY 2010) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	VA Organizations	Yes	Prime Vendor, Purchase Card (including Fee Basis and Convenience Check), Fleet, and Centrally Billed Travel data. Purpose is for Credit Card Costing.	N/A	131VA047 Routine Uses, Privacy Act, and VA Directive 6500. Release of information is ONLY to approved sytem owners, users, administrators and programmers. Access to CCS web application is restricted to authorized users only.
Other Veteran Organization	No	No	N/A	N/A	N/A
Other Federal Government Agency	Internal Revenue Service	No	VA shares 1099 information with the Internal Revenue Service. This information may include: card holder name, address, SSN, TIN, or other identification number.	PII	External policy that guides release of information is the IRS requirement to complete the IRS 1099-Misc form, IRS Publication 1220. Internal policies in VA Directive 6500 and VA Directive 6502 are followed.
State Government Agency	No	No	N/A	N/A	N/A
Local Government Agency	No	No	N/A	N/A	N/A
Research Entity	No	No	N/A	N/A	N/A
Other Project / System	N/A	No	N/A	N/A	N/A
Other Project / System	N/A	No	NA	N/A	N/A
Other Project / System	NA	No	N/A	N/A	N/A

(FY 2010) PIA: Access to Records

Does the system gather information from another system?	Yes
Please enter the name of the system:	electronic file from US Bank

Per responses in Tab 4, does the system gather information from an individual?	No
If information is gathered from an individual, is the information provided:	☐ Through a Written Request ☐ Submitted in Person ☐ Online via Electronic Form

Is there a contingency plan in place to process information when the system is down?	Yes

(FY 2010) PIA: Secondary Use

Will PII data be included with any secondary use request?	No
if yes, please check all that apply:	☐ Drug/Alcohol Counseling ☐ Mental Health ☐ HIV ☐ Research ☐ Sickle Cell ☐ Other (Please Explain)

Describe process for authorizing access to this data.

Answer: N/A

(FY 2010) PIA: Program Level Questions

Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public?　　　　　　　　　　　　　No

If Yes, Please Specify:

Explain how collected data are limited to required elements:
Answer: See additional information below.

How is data checked for completeness?
Answer: See additional information below.

What steps or procedures are taken to ensure the data remains current and not out of date?
Answer: See additional information below.

How is new data verified for relevance, authenticity and accuracy?
Answer: See additional information below.

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)
Answer: CCS does not verify the data. CCS receives the data from the processing bank through Daily card transaction information.

(FY 2010) PIA: Retention & Disposal

What is the data retention period?
Answer: Records are retained in inactive storage for 1 year after the close of the fiscal year, then retained on tape for the remainder of the 6 years and 3 months as required by GRS 6, Item 1a.

Explain why the information is needed for the indicated retention period?
Answer: NARA rules and GAO Auditing purposes

What are the procedures for eliminating data at the end of the retention period?
Answer: Destruction is accomplished based on GRS and SF Form 135 disposition date

Where are these procedures documented?
Answer: VA Handbook 6300.1, 7d. And NIST 800-88 Appendix -1 Table A. Also identified on Financial Accounting Service Record File Plan.

How are data retention procedures enforced?
Answer: Records Officer and Records Liasion Officer comply with VA Handbook 6300.1, Chap 6, Section 3. We are also finalizing procedures to classify categories of documents stored electronically with appropriate disposition. Once completed records that have met their retention preriod will automatically be flagged for disposition using approved NARA GRS and MP-4, Part X VA RCS for Office of Budget and Finance.

Has the retention schedule been approved by the National Archives and Records Administration (NARA)　　　　　　　　　　　　　Yes

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer: None.

(FY 2010) PIA: Children's Online Privacy Protection Act (COPPA)

Will information be collected through the internet from children under age 13?   No

If Yes, How will parental or guardian approval be obtained?

Answer:

(FY 2010) PIA: Security

Is the system/application/program following IT security
Requirements and procedures required by federal law and
policy to ensure that information is appropriately secured.

Yes

Has the system/application/program conducted a risk
assessment, identified appropriate security controls to protect
against that risk, and implemented those controls..

Yes

Is security monitoring conducted on at <u>least</u> a quarterly basis to
ensure that controls continue to work properly, safeguarding
the information?

Yes

Is security testing conducted on at <u>least</u> a quarterly basis to
ensure that controls continue to work properly, safeguarding
the information?

Yes

Are performance evaluations conducted on at <u>least</u> a quarterly
basis to ensure that controls continue to work properly,
safeguarding the information?

Yes

If 'No' to any of the 3 questions above, please describe why:
Answer: N/A

Is adequate physical security in place to protect against
unauthorized access?

Yes

If 'No' please describe why:
Answer: N/A

Explain how the project meets IT security requirements and
procedures required by federal law.
Answer: CCS follows all the VA mandated IT security
requirements and procedures required by federal law. CCS
servers reside in an access restricted secure location protected
by physical access restrictions and environmental protection
control measures. User access to the database is limited to as
needed basis. The database is further protected by soft wares
such as Intrusion Prevention and Detection System, Network
Scanner and Patch Management, and Firewall. Further, CCS is
protected by administrative controls such as Security Plans,
Rules of Behavior, and Procedures for establishing user
accounts

Explain what security risks were identified in the security
assessment? *(Check all that apply)*

☐ Air Conditioning Failure	☐ Hardware Failure
☑ Chemical/Biological Contamination	☑ Malicious Code
☐ Blackmail	☑ Computer Misuse
☐ Bomb Threats	☐ Power Loss
☐ Cold/Frost/Snow	☑ Sabotage/Terrorism
☐ Communications Loss	☑ Storms/Hurricanes
☑ Computer Intrusion	☐ Substance Abuse
☐ Data Destruction	☐ Theft of Assets
☐ Data Disclosure	☐ Theft of Data
☑ Data Integrity Loss	☐ Vandalism/Rioting
☐ Denial of Service Attacks	☐ Errors (Configuration and Data Entry)
☐ Earthquakes	☐ Burglary/Break In/Robbery
☑ Eavesdropping/Interception	☐ Identity Theft
☑ Fire (False Alarm, Major, and Minor)	☑ Fraud/Embezzlement
☑ Flooding/Water Damage	

Answer: (Other Risks)

Explain what security controls are being used to mitigate these
risks. *(Check all that apply)*

☑ Risk Management	☑ Audit and Accountability
☑ Access Control	☑ Configuration Management
☑ Awareness and Training	☑ Identification and Authentication
☑ Contingency Planning	☐ Incident Response
☑ Physical and Environmental Protection	☑ Media Protection
☑ Personnel Security	
☑ Certification and Accreditation Security Assessments	

Answer: (Other Controls)

PIA: PIA Assessment

Identify what choices were made regarding the project/system
or collection of information as a result of performing the PIA.
Answer: Reconsideration of collection information in CCS and
additional security controls to mitigate the risks listed above

Availability Assessment: If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization?
(Choose One)

☐ The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.

☑ The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.

☐ The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

Integrity Assessment: If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization?
(Choose One)

☐ The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.

☑ The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.

☐ The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

Confidentiality Assessment: If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization?
(Choose One)

☐ The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.

☑ The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.

☐ The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

The controls are being considered for the project based on the selections from the previous assessments?

The VA's risk assessment validates the security control set and determines if any additional controls are needed to protect agency operations. Many of the security controls such as contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls are common security controls used throughout the VA. Our overall security controls follow NIST SP800-53 moderate impact defined set of controls. The system owner is responsible for any system-specific issues associated with the implementation of this facility' common security controls. These issues are identified and described in the system security plans for the individual information systems.

Please add additional controls:

(FY 2010) PIA: Additional Comments

Add any additional comments on this tab for any question in the form you want to comment on.
Please indicate the question you are responding to and then add your comments.

Tab 2 - System Identification - Description of System (Continued)

to the VA FSC File Transfer Protocol (FTP) firewall server located in a demilitarized zone (DMZ) environment using the FTP over the Internet for further processing. These transactions are loaded into the Credit Card System database and are posted to the VA's Financial Management System (FMS) and IFCAP. VA cardholders use the CCS web application to reconcile transactions or reallocate transactions. The CCS generates several daily, weekly and monthly reports for use by FSC analysts.

The CCS application supports the FSC mission of providing high quality, cost-effective information technology business solutions, under franchise fund authority, to VA and other government agencies. The CCS application provides a full complement of application programs necessary to accommodate customer needs for processing the payment of financial transactions.

Information Technology (IT) services, supporting the CCS application, include security and management features that reside on the FSC Network. This includes, but is not limited to: local- and wide-area network (LAN/WAN) management, facilities for data warehousing, archival storage, fully supported electronic commerce/electronic data interchange, comprehensive disaster recovery programs, output preparation and distribution, full-service help desk, and user interfaces/support features.

Explain what minor application that are associated with your installation? *(Check all that apply)*

Records Locator System	Education Training Website	Appraisal System
Veterans Assistance Discharge System (VADS)	VR&E Training Website	Web Electronic Lender Identification
LGY Processing	VA Reserve Educational Assistance Program	CONDO PUD Builder
Loan Service and Claims	Web Automated Verification of Enrollment	Centralized Property Tracking System
LGY Home Loans	Right Now Web	Electronic Appraisal System
Search Participant Profile (SPP)	VA Online Certification of Enrollment (VA-ONCE)	Web LGY
Control of Veterans Records (COVERS)	Automated Folder Processing System (AFPS)	Access Manager
SHARE	Personal Computer Generated Letters (PCGL)	SAHSHA
Modern Awards Process Development (MAP-D)	Personnel Information Exchange System (PIES)	VBA Data Warehouse
Rating Board Automation 2000 (RBA2000)	Rating Board Automation 2000 (RBA2000)	Distribution of Operational Resources (DOOR)
State of Case/Supplemental (SOC/SSOC)	SHARE	Enterprise Wireless Messaging System (Blackberry)
Awards	State Benefits Reference System	VBA Enterprise Messaging System
Financial and Accounting System (FAS)	Training and Performance Support System (TPSS)	LGY Centralized Fax System
Eligibility Verification Report (EVR)	Veterans Appeals Control and Locator System (VACOLS)	Review of Quality (ROQ)
Automated Medical Information System (AMIS)290	Veterans On-Line Applications (VONAPP)	Automated Sales Reporting (ASR)
Web Automated Reference Material System (WARMS)	Automated Medical Information Exchange II (AIME II)	Electronic Card System (ECS)
Automated Standardized Performace Elements Nationwide (ASPEN)	Committee on Waivers and Compromises (COWC)	Electronic Payroll Deduction (EPD)
Inquiry Routing Information System (IRIS)	Common Security User Manager (CSUM)	Financial Management Information System (FMI)
National Silent Monitoring (NSM)	Compensation and Pension (C&P) Record Interchange (CAPRI)	Purchase Order Management System (POMS)
Web Service Medical Records (WebSMR)	Control of Veterans Records (COVERS)	Veterans Canteen Web
Systematic Technical Accuracy Review (STAR)	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)	Inventory Management System (IMS)
Fiduciary STAR Case Review	Fiduciary Beneficiary System (FBS)	Synquest
Veterans Exam Request Info System (VERIS)	Hearing Officer Letters and Reports System (HOLAR)	RAI/MDS
Web Automated Folder Processing System (WAFPS)	Inforce	ASSISTS
Courseware Delivery System (CDS)	Awards	MUSE
Electronic Performance Support System (EPSS)	Actuarial	Bbraun (CP Hemo)
Veterans Service Representative (VSR) Advisor	Insurance Self Service	VIC
Loan Guaranty Training Website	Insurance Unclaimed Liabilities	BCMA Contingency Machines
C&P Training Website	Insurance Online	Script Pro

Explain any minor application that are associated with your installation that does not appear in the
list above. Please provide name, brief description, and any comments you may wish to include.

	Name		Description	Comments
Minor app #1			Is PII collected by this min or application?	
			Does this minor application store PII?	
			If yes, where?	
			Who has access to this data?	

	Name		Description	Comments
Minor app #2			Is PII collected by this min or application?	
			Does this minor application store PII?	
			If yes, where?	
			Who has access to this data?	

	Name		Description	Comments
Minor app #3			Is PII collected by this min or application?	
			Does this minor application store PII?	
			If yes, where?	
			Who has access to this data?	

Baker System	Veterans Assistance Discharge System (VADS)
Dental Records Manager	VBA Training Academy
Sidexis	Veterans Service Network (VETSNET)
Priv Plus	Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)
Mental Health Asisstant	BIRLS
Telecare Record Manager	Centralized Accounts Receivable System (CARS)
Omnicell	Compensation & Pension (C&P)
Powerscribe Dictation System	Corporate Database
EndoSoft	Control of Veterans Records (COVERS)
Compensation and Pension (C&P)	Data Warehouse
Montgomery GI Bill	INS - BIRLS
Vocational Rehabilitation & Employment (VR&E) CH 31	Mobilization
Post Vietnam Era educational Program (VEAP) CH 32	Master Veterans Record (MVR
Spinal Bifida Program Ch 18	BDN Payment History
C&P Payment System	
Survivors and Dependents Education Assistance CH 35	
Reinstatement Entitelment Program for Survivors (REAPS)	
Educational Assistance for Members of the Selected Reserve Program CH 1606	
Reserve Educational Assistance Program CH 1607	
Compensation & Pension Training Website	
Web-Enabled Approval Management System (WEAMS)	
FOCAS	
Work Study Management System (WSMS)	
Benefits Delivery Network (BDN)	
Personnel and Accounting Integrated Data and Fee Basis (PAID)	
Personnel Information Exchange System (PIES)	
Rating Board Automation 2000 (RBA2000)	
SHARE	
Service Member Records Tracking System	

Explain what minor application that are associated with your installation? *(Check all that apply)*

ACCOUNTS RECEIVABLE	DRUG ACCOUNTABILITY	INPATIENT MEDICATIONS
ADP PLANNING (PLANMAN)	DSS EXTRACTS	INTAKE/OUTPUT
ADVERSE REACTION TRACKING	EDUCATION TRACKING	INTEGRATED BILLING
ASISTS	EEO COMPLAINT TRACKING	INTEGRATED PATIENT FUNDS
AUTHORIZATION/SUBSCRIPTION	ELECTRONIC SIGNATURE	INTERIM MANAGEMENT SUPPORT
AUTO REPLENISHMENT/WARD STOCK	ENGINEERING	KERNEL
AUTOMATED INFO COLLECTION SYS	ENROLLMENT APPLICATION SYSTEM	KIDS
AUTOMATED LAB INSTRUMENTS	EQUIPMENT/TURN-IN REQUEST	LAB SERVICE
AUTOMATED MED INFO EXCHANGE	EVENT CAPTURE	LETTERMAN
BAR CODE MED ADMIN	EVENT DRIVEN REPORTING	LEXICON UTILITY
BED CONTROL	EXTENSIBLE EDITOR	LIBRARY
BENEFICIARY TRAVEL	EXTERNAL PEER REVIEW	LIST MANAGER
CAPACITY MANAGEMENT - RUM	FEE BASIS	MAILMAN
CAPRI	FUNCTIONAL INDEPENDENCE	MASTER PATIENT INDEX VISTA
CAPACITY MANAGEMENT TOOLS	GEN. MED. REC. - GENERATOR	MCCR NATIONAL DATABASE
CARE MANAGEMENT	GEN. MED. REC. - I/O	MEDICINE
CLINICAL CASE REGISTRIES	GEN. MED. REC. - VITALS	MENTAL HEALTH
CLINICAL INFO RESOURCE NETWORK	GENERIC CODE SHEET	MICOM
CLINICAL MONITORING SYSTEM	GRECC	MINIMAL PATIENT DATASET
CLINICAL PROCEDURES	HEALTH DATA & INFORMATICS	MYHEALTHEVET
CLINICAL REMINDERS	HEALTH LEVEL SEVEN	Missing Patient Reg (Original) A4EL
CMOP	HEALTH SUMMARY	NATIONAL DRUG FILE
CONSULT/REQUEST TRACKING	HINQ	NATIONAL LABORATORY TEST
CONTROLLED SUBSTANCES	HOSPITAL BASED HOME CARE	NDBI
CPT/HCPCS CODES	ICR - IMMUNOLOGY CASE REGISTRY	NETWORK HEALTH EXCHANGE
CREDENTIALS TRACKING	IFCAP	NOIS
DENTAL	IMAGING	NURSING SERVICE
DIETETICS	INCIDENT REPORTING	OCCURRENCE SCREEN
DISCHARGE SUMMARY	INCOME VERIFICATION MATCH	ONCOLOGY
DRG GROUPER	INCOMPLETE RECORDS TRACKING	ORDER ENTRY/RESULTS REPORTING

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

	Name		Description	Comments

Minor app #1

Is PII collected by this min or application?

Does this minor application store PII?

If yes, where?	

Who has access to this data?	

	Name		Description	Comments

Minor app #2

Is PII collected by this min or application?

Does this minor application store PII?

If yes, where?	

Who has access to this data?	

	Name		Description	Comments

Minor app #3

Is PII collected by this min or application?

Does this minor application store PII?

If yes, where?	

Who has access to this data?	

OUTPATIENT PHARMACY	SOCIAL WORK
PAID	SPINAL CORD DYSFUNCTION
PATCH MODULE	SURGERY
PATIENT DATA EXCHANGE	SURVEY GENERATOR
PATIENT FEEDBACK	TEXT INTEGRATION UTILITIES
PATIENT REPRESENTATIVE	TOOLKIT
PCE PATIENT CARE ENCOUNTER	UNWINDER
PCE PATIENT/IHS SUBSET	UTILIZATION MANAGEMENT ROLLUP
PHARMACY BENEFITS MANAGEMENT	UTILIZATION REVIEW
PHARMACY DATA MANAGEMENT	VA CERTIFIED COMPONENTS - DSSI
PHARMACY NATIONAL DATABASE	VA FILEMAN
PHARMACY PRESCRIPTION PRACTICE	VBECS
POLICE & SECURITY	VDEF
PROBLEM LIST	VENDOR - DOCUMENT STORAGE SYS
PROGRESS NOTES	VHS&RA ADP TRACKING SYSTEM
PROSTHETICS	VISIT TRACKING
QUALITY ASSURANCE INTEGRATION	VISTALINK
QUALITY IMPROVEMENT CHECKLIST	VISTALINK SECURITY
QUASAR	VISUAL IMPAIRMENT SERVICE TEAM ANRV
RADIOLOGY/NUCLEAR MEDICINE	VOLUNTARY TIMEKEEPING
RECORD TRACKING	VOLUNTARY TIMEKEEPING NATIONAL
REGISTRATION	WOMEN'S HEALTH
RELEASE OF INFORMATION - DSSI	CARE TRACKER
REMOTE ORDER/ENTRY SYSTEM	
RPC BROKER	
RUN TIME LIBRARY	
SAGG	
SCHEDULING	
SECURITY SUITE UTILITY PACK	
SHIFT CHANGE HANDOFF TOOL	

Add any information concerning minor applications that may be associated with your system. Please indicate the name of the minor application, a brief description, and any comments you may wish to include. If you have more than 3 minor applications please copy then below sections as many times as needed.

	Name		Description	Comments
Minor app #1				

Is PII collected by this min or application?

Does this minor application store PII?

If yes, where?

Who has access to this data?

	Name		Description	Comments
Minor app #2				

Is PII collected by this min or application?

Does this minor application store PII?

If yes, where?

Who has access to this data?

	Name		Description	Comments
Minor app #3				

Is PII collected by this min or application?

Does this minor application store PII?

If yes, where?

Who has access to this data?

(FY 2010) PIA: Final Signatures

Facility Name: 0

Title:	Name:	Phone:	Email:
Privacy Officer:	Cathy Brean	512-460-5175	cathy.brean@va.gov

Digital Signature Block

Information Security Officer:	Krystal Johle	512-460-5043	krystal.johle@va.gov

Digital Signature Block

Chief Information Officer:	Larry Sherman	512-460-5300	larry.sherman@va.gov

Digital Signature Block

Person Completing Document:	Lori Thomas	512-460-5189	lori.thomas2@va.gov

Digital Signature Block

System / Application / Program Manager:	Ed Niedzielski	512-460-3079	edward.niedzielski@va.gov

Digital Signature Block

Date of Report: 12/17/2009
OMB Unique Project Identifier   None
Project Name   OM>FSC>CCS>